Dan Roelker

Program Manager, Information Innovation Office

Scaling Cyberwarfare

DARPA Cyber Colloquium

Arlington, VA

November 7, 2011

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE
07 NOV 2011

2. REPORT TYPE

3. DATES COVERED
00-00-2011 to 00-00-2011

4. TITLE AND SUBTITLE
Scaling Cyberwarfare

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Defense Advanced Research Projects Agency (DARPA),Information Innovation Office,3701 North Fairfax Drive,Arlington,VA,22203-1714

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the Colloquium on Future Directions in Cyber Security on November 7, 2011, Arlington, VA.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**7**	

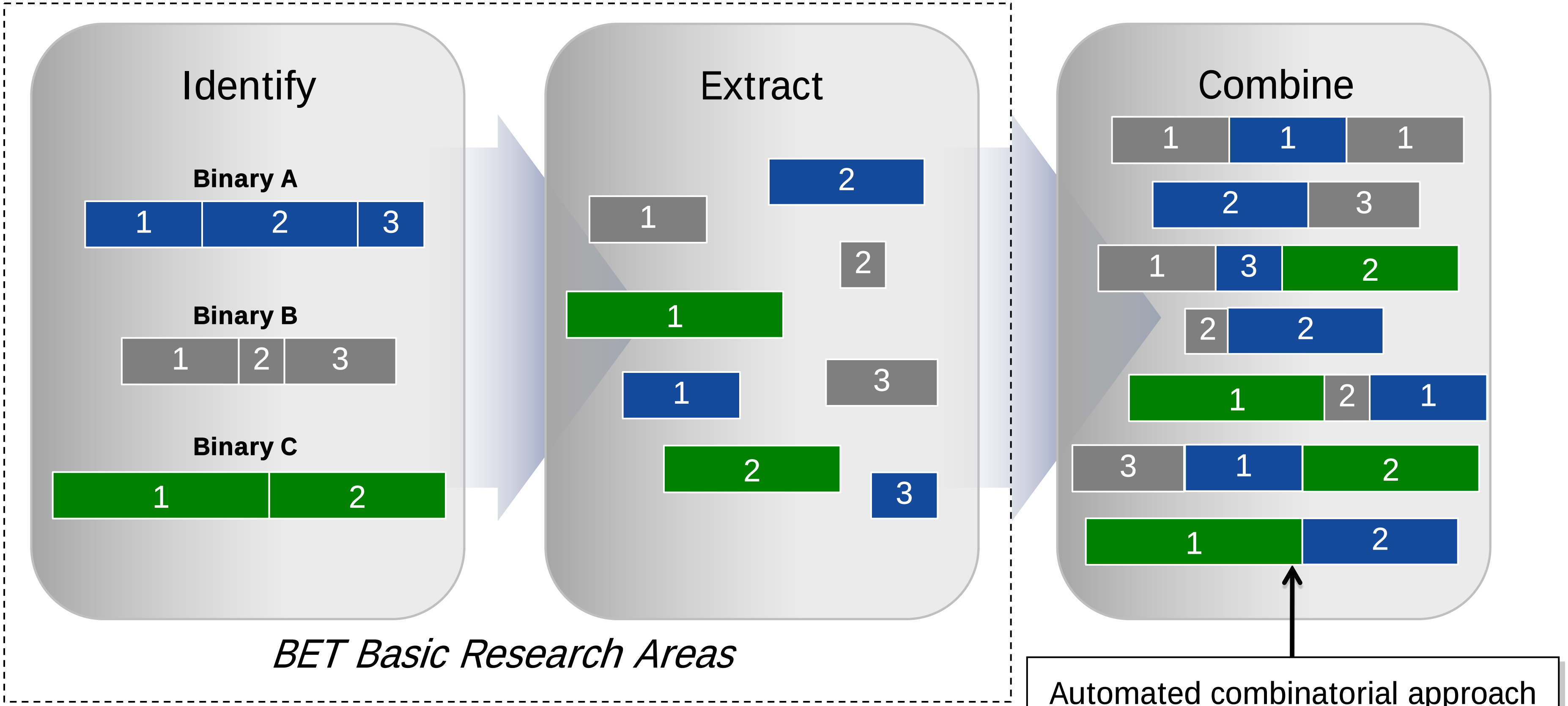
Cyberartisan production doesn't scale

All cybertools have a limited shelf-life and operational relevance

	Cyberartisan	*Automation*
Skill	Individual	Technology-based
Level of effort	Manually intensive	Mass produced
Cost/Benefit	"Too big to fail"	Cost effective

Approved for Public Release, Distribution Unlimited.

Program: Binary Executable Transforms (BET)



Automated combinatorial approach to software development given requirements could provide novel outcomes and diverse binary sets

BET identifies and extracts functional components from binary executables with potential for reusing components in new combinations

Hacker vs. Hacker approach doesn't scale

Skill Level

Not everyone can be the cyber equivalent of a Navy SEAL

Scaling Limitations
Force size
Execution speed
Tactical depth

We don't win wars by out-hiring an adversary, we win through technology

Limitations to the Hacker vs. Hacker approach

Cyberwarfare is executed at the speed of light . . .

Force Size Limitations
#of people trained per year
# of people to execute a mission

Execution Speed Limitations
Speed of planning process
Speed of mission operation

Tactical Depth Limitations
Real-time move-counter-move
Multi-phase mission strategy

we need breakthroughs in technology to accomplish this goal

Pillars of Foundational Cyberwarfare

Exploitation Research

automation techniques, defeating formal methods, high-fidelity emulation

Network Analysis

on-demand topology, infrastructure capability, platform positioning

Planning and Execution

assured and automated execution, large-scale analytics, distributed planning

Cyberwarfare Platform Development

Visualization

new interfaces, adaptable views, large-scale data representation

Ideas, thoughts, code? daniel.roelker@darpa.mil